

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-157554

(43)Date of publication of application : 31.05.2002

(51)Int.Cl. G06K 17/00

G06F 9/46

G06F 12/14

G06K 19/073

(21)Application number : 2001-220865 (71)Applicant : FUJITSU LTD

(22)Date of filing : 23.07.2001 (72)Inventor : KURITA YUKIYOSHI

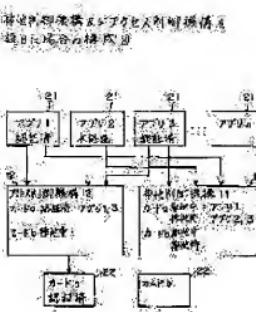
(30)Priority

Priority number : 2000269096 Priority date : 05.09.2000 Priority country : JP

(54) SYSTEM FOR MANAGING ACCESS OF SMART CARD, SHARING METHOD
AND STORAGE MEDIUM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide an access management system and a managing method for a smart card, which give an authentication permission to each application (process) in regard to accesses by a plurality of applications.



SOLUTION: The applications 21 including a plurality of pieces of access processing to the smart card make an exclusion acquisition request to an exclusion control mechanism 11 at the time of making an access request to the smart card 22 in each access processing and requests access to an access control mechanism 12 when the applications 21 obtain exclusion.

The mechanism 12 requests an input of a PIN(personal identification number) when the concerned application 21 is not authenticated, and allows the application 21 to access the smart card 22 when the application 21 has already obtained authentication. The application 21 performs exclusion acquisition request/release in an access processing unit.

CLAIMS

[Claim(s)]

[Claim 1] It is the access control system of the smart card which manages access to the smart card by two or more applications. If the logical channel [finishing / a logical channel / exclusion acquisition] exists in this smart card with other applications to the exclusion acquisition demand to the smart card from application As opposed to the access request to said smart card from the exclusive control means made finishing [exclusion acquisition of this application] and the application [finishing / application / exclusion acquisition] The access control system characterized by equipping the application [finishing / application / this exclusion acquisition] with an access control means to permit access to this smart card when the application [finishing / application / this exclusion acquisition] is already attested from this smart card.

[Claim 2] Said exclusive control means is an access control system according to claim 1 characterized by registering into a queue the application which performed this exclusion acquisition demand if the logical channel [finishing / a logical channel / exclusion acquisition] does not exist in this smart card with other applications to the exclusion acquisition demand to the smart card from application.

[Claim 3] Said access-control means is an access control system according to claim 1 or 2 characterized by refusing the demand of this application when having not attested the application which gained said exclusion from said smart card to said access request.

[Claim 4] Said access-control means is claim 1 characterized by changing the application [finishing / application / authentication] into un-attesting by this ***** smart card when said smart card is extracted from a smart card reader thru/or an access control system given in any 1 of 3.

[Claim 5] Said application is claim 1 characterized by giving said exclusion acquisition demand to said exclusive control means at the time of initiation of each access, and carrying out the notice of discharge of exclusion to said exclusive control means at the time of termination of this access of each when carrying out multiple-times access at said smart card thru/or an access control system given in any 1 of 4.

[Claim 6] Said exclusive control means is an access control system according to claim 5 to which this smart card is characterized by supposing finishing [exclusion acquisition of the application which registers into a queue the application which performed this exclusion acquisition demand when it was already exclusion acquisition ending, and is registered into said queue to the notice of discharge of the exclusion from said application] with other applications to the exclusion acquisition demand to the smart card from application.

[Claim 7] Said access-control means is claim 1 to which this authentication discharge is characterized by requiring authentication discharge of this smart card by this smart card at the time from the last application [finishing / the application / authentication] from application to the notice of authentication discharge of a smart card thru/or an access control system given in any 1 of 6.

[Claim 8] It is the share approach of the smart card which manages access to the smart card by two or more applications. If the logical channel [finishing / a logical channel / exclusion acquisition] exists in this smart card with other applications to the exclusion acquisition demand to the smart card from application As opposed to the access request to said smart card from the application [finishing / finishing / exclusion acquisition of this application / is supposed and / application / exclusion acquisition] The share approach characterized by permitting access to this smart card to the application

[finishing / application / this exclusion acquisition] when the application [finishing / application / this exclusion acquisition] is already attested from this smart card.

[Claim 9] The application are the application contain two or more access processings by one smart card, or its library, carry out an exclusion acquisition demand to two or more access processings, respectively at the time of initiation of this access processing, give a discharge notice in exclusion and carry out carrying out an authentication demand to the smart card carry out this access processing only at the time of processing of the beginning of the access processings of said plurality as the description at the time of termination of each access processing, respectively, or its library.

[Claim 10] When used by the information processor in which two or more applications carry out juxtaposition actuation, If the logical channel [finishing / a logical channel / exclusion acquisition] exists in this smart card with other applications to the exclusion acquisition demand to the smart card from application As opposed to the access request to said smart card from the application [finishing / finishing / exclusion acquisition of this application / is supposed and / application / exclusion acquisition] When the application [finishing / application / this exclusion acquisition] is already attested from this smart card, The record medium which said information processor which memorized the program to which it makes it carry out to said information processor to permit access to this smart card to the application [finishing / application / this exclusion acquisition] can read.

[Claim 11] When it performs with the information processor in which two or more applications carry out juxtaposition actuation, If the logical channel [finishing / a logical channel / exclusion acquisition] exists in this smart card with other applications to the exclusion acquisition demand to the smart card from application As opposed to the access request to said smart card from the application [finishing / finishing / exclusion acquisition of this application / is supposed and / application / exclusion acquisition] The program to which it makes it carry out to said information processor to permit access to this smart card to the application [finishing / application / this exclusion acquisition] when the application [finishing / application / this exclusion acquisition] is already attested from this smart card.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention] This invention relates to the access control of the smart card at the time of [which is depended on two or more processes of the data on a smart card] sharing.

[0002]

[Description of the Prior Art] The use to various fields from the data of a very big capacity being memorizable as compared with the magnetic card used conventionally etc. is considered, or the smart card is put in practical use.

[0003] Moreover, since the smart card equips the interior with CPU with memory and is accessed to the data in memory through this CPU, by making authentication processing perform to CPU at the time of access, high security nature can be realized compared with the conventional magnetic card, and this point also serves as a merit of a smart card.

[0004] The smart card has a security function by PIN (Personal Identification Number), and collates PIN by this function, and only when attested, controlling to be able to access the confidential information in a card is possible. The authentication by this PIN is the so-called password input method, the user using a smart card enters a password as PIN, and it compares within the password which has memorized this in a smart card, and a card, and when in agreement, access to an in-house data is permitted.

[0005] Access to a smart card is performed through the logical channel which a smart card has, and an authentication demand is given to a logical channel. And the smart card holds the conditions about security, such as an authentication condition by PIN, for every logical channel of this.

[0006] Drawing 15 shows the logical construction inside the smart card seen from application. Within the smart card, data are managed by the configuration of a tree structure and DF (Delicated File) is prepared in the unit for every application used for the lower layer of DIR in the most significant etc. And in each DF, EF (Elementary File) holding actual data is stored. In case data are accessed from a smart card, after application sends the positioning information which shows the location of the data accessed first and moves an access location to the target EF, it performs the readout/writing of data from the EF. Moreover, each channel holds the current access location as status information.

[0007]

[Problem(s) to be Solved by the Invention] The usage which uses a current smart card for coincidence with two or more applications is examined. For example, when the PKI (Public Key Instructure) system which used the public key cryptosystem as the base is built and two or more applications are working by computer on this system, it is

considered as one operation of a current smart card that each application uses a smart card for the security authentication by a digital signature etc.

[0008] In this case, two or more applications on the computer which connected the smart card will share a smart card. And since the number of the logical channels which one smart card has is about at most two, when making much applications access to the same card, the need that two or more applications share one logical channel comes out. For simplification of explanation, the following explanation in a **** specification is premised on one application consisting of one process, is synonymous with a process and uses the word "application." Usually, although one application consists of one process in many cases, if application is replaced with a process and considered even when it consists of multiple processes, the following explanation is fundamentally the same.

[0009] By the security method of the present smart card, if PIN authentication is performed to a logical channel with one application and an access permission is obtained, from the logical channel, not only the application that received authentication but other applications will be able to be henceforth accessed until authentication is canceled.

[0010] If it considers sharing the same information on one card between two or more applications from a viewpoint of security, the direction will become firmer [security level] having performed authentication by PIN for each application of every. However, in the access control to the present smart card, since authentication is performed for every logical channel and an authentication condition (was the access permission given or not?) is held at each logical channel, when two or more applications share one logical channel, if one application performs authentication by PIN and obtains an access permission, access of other applications to a card from the logical channel will be attained, without receiving authentication by PIN.

[0011] Moreover, when two or more applications share a logical channel although the writing/readout of data are performed after transmitting positioning information to a logical channel and moving an access location in case each application accesses the data in a card as mentioned above, as for each application, grasp of the access location of KARENTO becomes difficult.

[0012] In view of the above-mentioned trouble, this invention makes it a technical problem to offer the access control system and management method of the smart card which gives authentication authorization to each application (process) of every to access by two or more applications (process) by carrying out unitary management of the authentication condition to a smart card. Moreover, let it be a technical problem to offer the access control system and management method which are realized without

enlarging the overhead according authentication of each application (process) of every to authentication processing.

[0013]

[Means for Solving the Problem] In order to solve the above-mentioned trouble, the access control system of the smart card by this invention manages access to the smart card by two or more applications, and is equipped with a exclusive control means and an access-control means.

[0014] A exclusive control means will presuppose finishing [exclusion acquisition of this application], if the logical channel [finishing / a logical channel / exclusion acquisition] exists in this smart card with other applications to the exclusion acquisition demand to the smart card from application. Moreover, the above-mentioned exclusive control means registers into a queue the application which performed this exclusion acquisition demand, if the logical channel [finishing / a logical channel / exclusion acquisition] does not exist in this smart card with other applications to the exclusion acquisition demand to the smart card from application.

[0015] An access-control means permits access to this smart card to the application [finishing / application / this exclusion acquisition], when the application [finishing / application / this exclusion acquisition] is already attested from this smart card to the access request to the above-mentioned smart card from the application [finishing / application / exclusion acquisition]. Moreover, an access-control means requires the input of PIN of this application, when having not attested the application which gained the above-mentioned exclusion from the above-mentioned smart card to the above-mentioned access request. Authentication of the smart card by each application was performed through this access-control means, and the access-control means grasps the authentication relation between each application and a smart card.

[0016] According to this invention, since exclusive control to a smart card is performed by the exclusive control means, even if it shares a smart card with two or more applications, authentication for every application is enabled.

[0017] Moreover, it is judged by the access-control means whether it is finishing [authentication of the application which performed each access request], and since an access permission is given without performing authentication processing when it is authentication ending, the count of authentication processing is reducible.

[0018]

[Embodiment of the Invention] One operation gestalt of this invention is explained below, referring to a drawing. In order to give authentication authorization for every application, it controls exclusively to a smart card (it is a logical channel when a smart

card has two or more logical channels), and while one attested application is using the smart card, the application needs to monopolize a card (or logical channel), and needs to inhibit access from other applications. In addition, with the following operation gestalten, each smart card is taken as a configuration equipped with one logical channel for explanation simplification. In addition, when a smart card is equipped with two or more logical channels, exclusive control explained below is performed per logical channel.

[0019] Drawing 1 establishes a exclusive control device and shows the case where the exclusive operation of the application which accesses a smart card is performed. In drawing 1, in case the exclusive control device 11 is established between two or more applications 21 and a smart card 22 and access is required from a smart card 22, each application 21 performs an exclusion acquisition demand to this exclusive control device 11, and the application 21 with which exclusion was obtained accesses it by monopolizing a smart card 22. The exclusive control device 11 of this drawing has managed the exclusion to access to two cards of Cards a and b. And three applications, an application 1, an application 2, and an application 3, 21 have published the access request to Card a, and the exclusive control device 11 is considered as exclusion acquisition to the application 1 of them, and it changes other applications 2 and 3 into the waiting state until Card a is released. The application 1 which gained exclusion performs the readout/writing of data, after performing PIN authentication to the logical channel of Card a. The application 21 besides during this period cannot be accessed to Card a. If processing of an application 1 is completed and Card a is released next, the application 2 which is in the waiting state will gain exclusion, and will access the data inside backward [which performed PIN authentication to Card a]. Thus, by establishing the exclusive control device 11, only one application which received authentication can be accessed to a smart card, and authentication for every application 21 can be realized.

[0020] Since in the case of the method by the configuration of this drawing 1, this smart card 22 is monopolized by this application 21 while one application 21 is using the smart card 22, other applications 21 will be in a waiting state until exclusion is canceled and a smart card 22 is released. Therefore, by this method, the parallel processing engine performance of two or more applications is bad, and user friendliness worsens very much -- the application in a waiting state is visible to the condition of having suspended long period processing and having hung-up.

[0021] There is a method which releases in detail the smart card 22 which application 21 monopolized as what avoids this when the access processing to a smart card 22 was

completed. By this method, when application 21 includes the access processing to the multiple-times smart card 22, exclusion acquisition / release to a smart card 22 are performed to the exclusive control device 11 for every access processing, and exclusive control is divided into eye the top.

[0022] The example of the exclusion acquisition / release to the smart card of each application by this method is shown in drawing 2. This drawing is what shows the example of access processing to the smart card of each application when three applications, an application 1, an application 2, and an application 3, 21 publish an access request to Card a like drawing 1. As for arrow-head ** from the exclusion acquisition demand in the exclusive control device 11 from each application 21, and the exclusive control device 11, arrow-head ** to the exclusive control among said drawing device 11 shows the notice of the exclusion acquisition to each application 21 from the exclusive control device 11. Moreover, PIN authentication processing according [a shadow area] to each application 21 and a half-tone-dot-meshing part show access processing to a smart card 22.

[0023] When the application 21 which gained exclusion cancels exclusion and does not release a smart card 22 until all processings are completed, an application 2 will be in a waiting state further to the location of 33 which processing completes [the application 1 which has already gained the exclusion to Card a] from the location of 31 in drawing 2 which gave the exclusion acquisition demand on Card a to the exclusive-control device 11 until processing of this application 2 completes an application 3 from the location of 32. However, since another application 21 to the period of which exclusion was canceled when application 21 divided exclusive control into eye the top for every access processing, as shown in this drawing can access Card a, the period which will be in the waiting state for exclusion acquisition, and processing stops becomes short, and the parallelism of processing improves.

[0024] Thus, if exclusive control is changed frequently, the period of the waiting state of each application will become short, and the parallelism of processing will improve. However, as shown in the slash section of drawing 2, each application will need to perform setup/discharge processing of an authentication condition at every change, and the overhead for it will become large. Moreover, since PIN is transmitted in case re-authorization of authentication is obtained, each application 21 will continue holding PIN and also produces the problem on security. In order to avoid this, if it is the configuration as which a user enters a password at every authentication processing, the overhead of authentication processing will become large further.

[0025] The configuration which took this point into consideration to drawing 3 is shown.

With the configuration of **drawing 3**, the exclusive operation of the application 21 with which the exclusive control device 11 accesses a smart card 22 is performed, establishing an accessor controller 12 between two or more applications 21 and a smart card 22 in addition to the exclusive control device 11, and carrying out unitary management of the authentication by the smart card 22 of each application 21 according to this accessor controller 12.

[0026] In case each application 21 requires access from a smart card 22, if it performs an exclusion acquisition demand to the exclusive control device 11 first and exclusion can be gained, it will request the authentication to a smart card 22 from an accessor controller 12 next. And if authentication is acquired, the data in a smart card 22 will be accessed.

[0027] An accessor controller 12 has an authentication status management table, and the authentication condition of each application and a smart card 22 is managed about between after application 21 makes initiation declaration of the authentication to a smart card 22 using this authentication status management table until it notifies discharge of authentication.

[0028] **Drawing 4** is drawing showing the example of a configuration of an authentication status management table. the table which uses an authentication status management table in order that the exclusive control device 11 may manage from which smart card 22 each application 21 has acquired authentication now -- it is -- an application -- identification information and attested card information are matched and memorized. an application -- what cannot operate application with this general identifier is used by not memorizing an identifier [meaning / for identifying each application 21], for example, identification information is added to each process at a process generate time, and the process ID which the kernel has managed is used for it. Or it is good also as a configuration whose accessor controller 12 carries out sequential generation addition of the identifier to the application 21 which performed the access request to access to a smart card.

[0029] **Drawing 4** has illustrated the case where the authentication condition of each application 21 over two smart cards 22 of Cards a and b is managed, and the card with which the application 21 is attested as attested card information to each application is recorded. In addition, the part of a blank shows that the smart card [finishing / to the application / attested card information / a smart card / authentication] does not exist. this drawing -- an application 1 -- Cards a and b -- finishing [both authentication] -- an application 2 and an application -- finishing [each n / un-attesting and an application 3 / a card a / authentication].

[0030] Each application 21 performs access to the authentication and the smart card 22 to a smart card 22 through an accessor controller 12. If there is an access request from application 21 to a smart card 22, if the application 21 investigates whether it is authentication ending to the smart card 22 which carried out the access request and has not attested to it with reference to an authentication status management table, the demand from application 21 will be refused, and the input of PIN will be required of application 21, and authentication processing with a smart card 22 will be performed. Moreover, if the application 21 is authentication ending, since application 21 has already obtained authentication authorization of the smart card 21, access to a smart card 21 will be permitted and it will be performed.

[0031] Drawing 5 is drawing having shown the flow of processing of the application 21 at the time of application 21 performing access to a smart card 22, the exclusive control device 11, and an accessor controller 12. This drawing makes the example the case where an application 1 accesses to Card a, and 1-23 under following explanation correspond with the number in drawing 5.

- 1) An application 1 performs an exclusion acquisition demand to the exclusive control device 11 in order to perform exclusion initiation to Card a.
- 2) To the demand from an application 1, the exclusive control device 11 investigates whether there is any application [finishing / exclusion acquisition] to Card a, and if other applications have already gained, it will register it into the queue of the waiting for exclusion. Moreover, if it is not exclusion acquisition settled, exclusion acquisition will be notified to an application 1.
- 3) An application 1 makes access initiation declaration to Card a to an accessor controller 12.
- 4) An accessor controller 12 registers an application 1 into an authentication status management table to access initiation declaration. And the input request of PIN is performed to an application 1. In addition, when the application 1 is making access initiation declaration to Card b, since the application 1 is already registered into the authentication status management table, it is not necessary to register it into an authentication status management table again by the access initiation declaration to Card a.
- 5) An application 1 demands the input of a password from a user, specifies PIN from a user's input, and requires the authentication to Card a.
- 6) The exclusive control device 11 notifies PIN to Card a, and makes an authentication check perform on Card a.
- 7) If authentication is acquired as a result of the authentication check according [an

accessor controller 12] to Card a, an application 1 will register that it is authentication ending into an authentication status management table at Card a.

- 8) An application 1 requires read-out/writing of the data to Card a from an accessor controller 12.
- 9) To read-out/write request from an application 1, an authentication status management table is searched, and if an application 1 is authentication ending, it will access the attested card a to Card a. If it has not attested, an error will be notified to an application 1.
- 10) When one access processing is completed and it cancels monopoly of Card a, an application 1 notifies discharge of exclusion to the exclusive control device 11.
- 11) The exclusive control device 11 deletes the exclusion acquisition to the card a of the application 1 registered, and if there is application 21 otherwise registered into the queue of the waiting for the exclusion to Card a, it will register exclusion acquisition of the application 21.
- 12) An application 1 performs processings other than the access processing to Card a after discharge of exclusion. Since the exclusion of Card a is released in the meantime, other applications 21 can use Card a.
- 13) An application 1 will give an exclusion acquisition demand to the exclusive control device 11, if the need for access to Card a arises again.
- 14) finishing [it investigates again whether the exclusive control device 11 has application / finishing / exclusion acquisition / to Card a like 2 to the demand from an application 1, and / other applications / exclusion acquisition 1 already .. it is not .. if .. notify exclusion acquisition to an application 1.
- 15) An application 1 requires read-out/writing of the data to Card a from an accessor controller 12.
- 16) An accessor controller 12 performs the again same processing as 9. Since it is registered into the authentication status management table by 7 at this time that an application 1 is authentication ending at Card a, card a hair KUSESU is performed as it is. The processing for a count [10-16] of the access processing to the card a in an application 1 is repeated henceforth.
- 17) If all access processings are completed, an application 1 will notify discharge for the authentication to Card a to an accessor controller 12.
- 18) An accessor controller 12 deletes information [finishing / card a authentication] from the application 1 of an authentication status management table.
- 19) An accessor controller 12 will require authentication discharge of Card a, if an authentication condition is held and the application 21 attested stops existing until the

application 21 otherwise attested by Card a stops existing in the authentication status management table 13. Thereby, the count of authentication processing with the same smart card is reducible.

20) An application 1 notifies the access termination to a smart card 22 to an accessor controller 12.

21) If the notice by 20 is received, an accessor controller 12 will delete an application 1 from an authentication status management table. When the application 1 has not ended access yet to other smart cards 22 at this time, an application 1 is not deleted from an authentication status management table.

22) An application 1 notifies discharge of the exclusion of Card a to the exclusive control device 11.

23) The exclusive control device 11 performs the again same processing as 11, and cancels exclusion.

[0032] Drawing 6 is drawing showing the processing to the smart card of each application by the configuration equipped with the exclusive control device 11 and accessor controller 12 of drawing 3. This drawing has shown processing of the same application 21 under the same premise as drawing 2 for the comparison. As compared with drawing 2, it is only that each application 21 is performing authentication processing according drawing 6 to PIN at the time of the access processing initiation to the very first card a, and discharge processing of the authentication at the time of the very last access processing termination to Card a as authentication processing, and the authentication processing for every access processing to the card a which was being performed is omitted by drawing 2. Therefore, as for each application 21, the part processing time to which authentication processing was abbreviated becomes short. Moreover, the period when the period which monopolizes Card a will also be in the state waiting for a part since only the part from which authentication processing was excluded becomes short is short, and each application 21 may end. Furthermore, since each application 21 should perform PIN authentication over a smart card 22 only once first, if authentication is acquired from a card, it can cancel PIN.

[0033] Drawing 7 is a flow chart which shows processing of the application 21 which accesses a smart card 22 by this system. In addition, although the device in which these processings are performed can also be considered as the configuration which gives application 21 directly, a general configuration takes the gestalt which realizes these processings as a library and includes this library in each application 21.

[0034] In case application 21 accesses a smart card 22, it requests exclusion acquisition to the exclusive control device 11 first (step S1), and waits for the response from the

exclusive control device 11. Consequently, processing will be ended if there is a notice of a purport which cannot gain exclusion from the exclusive control device 11 by a certain reason (steps S2 and NO).

[0035] If there is a notice of an exclusion acquisition success from the exclusive control device 11 to a request of exclusion acquisition (steps S2 and YES), initiation declaration of access to a smart card 22 will be made to an accessor controller 12 as step S3 next.

[0036] Access to this smart card 22 is access to the non-attested smart card 22, and since the authentication to a smart card 22 is required, when the input of PIN is required from an accessor controller 12 (step S4, YES), it checks by sending the password which the user entered as PIN as step S8 to an accessor controller 12, and requesting authentication processing. Processing is ended, if are attested as a result (step S9, YES), and processing will be moved to step S5, it will access to a smart card and it will not be attested (step S9, NO).

[0037] In step S4, since the further authentication processing does not have the need when this access is access to the smart card 22 which has already acquired authentication (step S4, NO), access to a smart card 22 is permitted as step S5, and read-out/writing of data are performed.

[0038] Termination of access processing of step S5 makes termination declaration of access to a smart card 22 to an accessor controller 12 as step S6. And as step S7, discharge of the exclusion to the smart card 22 is notified to the exclusive control device 11, and the access processing to a smart card 22 is ended.

[0039] Drawing 8 is a flow chart which shows processing of the exclusive control device 11 over the exclusion acquisition demand from application 21. If the exclusion acquisition demand to a smart card 22 from application 21 is, the exclusive control device 11 will judge whether it is exclusion acquisition ending as step S11 with the application 21 of others [smart card / 22 / of which exclusion acquisition was required] already. If exclusion acquisition by the application 21 besides the result is not performed (steps S11 and NO), it registers as finishing [exclusion acquisition of the smart card 22], exclusion acquisition is notified to the application 22 which required, and processing is ended.

[0040] Moreover, if other applications 21 are exclusion acquisition ending at step S11 (steps S11 and YES), this exclusion acquisition demand will be added to the waiting queue for exclusion as step S12, and processing will be ended.

[0041] Drawing 9 is a flow chart which shows processing of the exclusive control device 11 over the notice of discharge of the exclusion from application 21. If the notice of discharge of the exclusion from application 21 to a smart card 22 is received, the

exclusive control device 11 will delete the registration as step S21 the application 21 of whose has been exclusion gained, and will cancel exclusion.

[0042] And the waiting queue for exclusion is investigated, and if the application 21 which serves as waiting for exclusion to the smart card 22 of which exclusion was canceled exists (steps S22 and YES), after registering the exclusion acquisition to the smart card 22 of the application 21 registered into the head of the waiting queue for exclusion and dispatching a smart card 22, and if waiting does not exist in the waiting queue for exclusion (steps S22 and NO), processing is ended as it is.

[0043] Drawing 10 is a flow chart which shows the processing of an accessor controller 12 to the access request to the smart card 22 from application 21. To the access initiation declaration from application 21, as step S31, an accessor controller 12 registers application 21 into an authentication status management table, and registers an access request process to a smart card 22.

[0044] Drawing 11 is a flow chart which shows the processing of an accessor controller 12 to the access request to the smart card 22 from application 21. As for an accessor controller 12, with reference to an authentication status management table, the application 21 investigates whether it is already authentication settled from the smart card 22 of the access request point as step S41 to the access request from application 21. Consequently, if it is already authentication ending (steps S41 and YES), since the further authentication does not have the need, an access permission is notified to application 21 as step S45.

[0045] If the application 21 has not acquired authentication yet (steps S41 and NO), since it is necessary to perform authentication processing at step S41, the input of a password is required of application 21 as step S42, and the authentication check by PIN is requested to a smart card 22. Consequently, if authentication is acquired from a smart card 22, an access permission will be notified to application 21 as step S45 and authentication will not be acquired (steps S43 and NO), access disapproval is notified to application 21 and processing is ended.

[0046] Drawing 12 is drawing showing the structure of a system which uses the smart card in this operation gestalt. The access control system 40 which manages between the application 41 in this operation gestalt and smart cards 42 is constituted between the smart card reader 43 and the library 44 of each application 41, and is realized in the form mounted in OS as one function of OS.

[0047] Application 41 performed altogether the authentication processing and access processing to a smart card 42 through this access control system 40, and the access control system 40 grasps the exchange between each application 41 and a smart card 42.

Moreover, if the condition of the smart card reader 43 is also grasped, for example, a smart card 42 is extracted from the smart card reader 43, the access control system 40 investigates an authentication status management table, and if there is application which the card makes finishing [authentication], it will change it into un-attesting.

[0048] In addition, although the access control system 40 has composition which has separately the exclusive control device 11 and an accessor controller 12 in the interior, these are also realizable as one functional component. Moreover, on security, since two or more applications share an accessor controller and a exclusive control device, if it realizes in the kernel of OS, they can improve security more.

[0049] Drawing 13 is the system environment Fig. of an information processor when a computer program realizes the access control of the above-mentioned smart card in this operation gestalt. The information processor which mounted the smart card like drawing 13 CPU51, ROM, I/O devices (I/O) 54, such as main storage 52, an auxiliary storage unit 53, a display, and a keyboard, LAN and WAN by RAM, The network connection equipments 55, such as a modem which performs other information processors and network connections by a general circuit etc., a disk, It had the smart card reader 58 which the medium readers 56 and 1 which read the contents of storage from the portable record media 57, such as a magnetic tape, thru/or plurality are, and mounts the smart card 59, and these are equipped with the configuration mutually connected by the bus 60.

[0050] Moreover, in the information processing system of drawing 13, the program and data which are memorized by the record media 57, such as a magnetic tape, a floppy (trademark) disk, CD-ROM, and MO, with the medium reader 56 are read, and this is downloaded to main storage 52 or a hard disk 55. And each processing by this operation gestalt can be realized by software, when CPU51 performs this program and data.

[0051] Moreover, in this information processor, exchange of application software may be performed using the record media 57, such as a floppy disk. Therefore, this invention can also be constituted as a record medium 57 in which computer read-out for operating the gestalt of operation of above-mentioned this invention as a computer is possible, when used not only by the access control system and the share approach of a smart card but by computer.

[0052] In this case, as shown in drawing 14, the memory (RAM or hard disk) 75 grade for example, within the portable record medium 76 in which desorption is possible to the medium driving gears 77, such as CD-ROM and a floppy disk (or you may be MO, DVD, a removable hard disk, etc.), the storage means 72 (database etc.) in the equipments (server etc.) of the exterior transmitted by network circuit 73 course, or the body 74 of

an information processor 71 is contained in a "record medium." The program memorized by the portable record medium 76 and the storage means (database etc.) 72 is loaded to the memory 75 within a body 74 (RAM or hard disk), and is performed.

[0053] (Additional remark 1) It is the access control system of the smart card which manages access to the smart card by two or more applications. If the logical channel [finishing / a logical channel / exclusion acquisition] exists in this smart card with other applications to the exclusion acquisition demand to the smart card from application As opposed to the access request to said smart card from the exclusive control means made finishing [exclusion acquisition of this application] and the application [finishing / application / exclusion acquisition] The access control system characterized by equipping the application [finishing / application / this exclusion acquisition] with an access-control means to permit access to this smart card when the application [finishing / application / this exclusion acquisition] is already attested from this smart card.

[0054] (Additional remark 2) Said exclusive control means is an access control system given in the additional remark 1 characterized by registering into a queue the application which performed this exclusion acquisition demand if the logical channel [finishing / a logical channel / exclusion acquisition] does not exist in this smart card with other applications to the exclusion acquisition demand to the smart card from application.

[0055] (Additional remark 3) Said access-control means is an access control system the additional remark 1 characterized by refusing the demand of this application when having not attested the application which gained said exclusion from said smart card to said access request, or given in 2.

[0056] (Additional remark 4) Said access-control means is an access control system the additional remark 1 characterized by managing the authentication relation between application and a smart card using the process ID of this application thru/or given in any 1 of 3.

[0057] (Additional remark 5) Said access-control means is an access control system the additional remark 1 characterized by changing the application [finishing / application / authentication] into un-attesting by this ***** smart card when said smart card is extracted from a smart card reader thru/or given in any 1 of 4.

[0058] (Additional remark 6) Said application is an access control system the additional remark 1 characterized by giving said exclusion acquisition demand to said exclusive control means at the time of initiation of each access, and carrying out the notice of discharge of exclusion to said exclusive control means at the time of termination of this

access of each when carrying out multiple-times access at said smart card thru/or given in any 1 of 5.

[0059] (Additional remark 7) Said exclusive control means is an access control system given in the additional remark 6 to which this smart card considers supposing finishing [exclusion acquisition of the application which registers into a queue the application which performed this exclusion acquisition demand when it was already exclusion acquisition ending, and is registered into said queue to the notice of discharge of the exclusion from said application] as the description with other applications to the exclusion acquisition demand to the smart card from application.

[0060] (Additional remark 8) Said access-control means is an access control system the additional remark 1 to which this authentication discharge is characterized by requiring authentication discharge of this smart card by this smart card at the time from the last application [finishing / the application / authentication] from application to the notice of authentication discharge of a smart card thru/or given in any 1 of 7.

[0061] (Additional remark 9) It is the share approach of the smart card which manages access to the smart card by two or more applications. If the logical channel [finishing / a logical channel / exclusion acquisition] exists in this smart card with other applications to the exclusion acquisition demand to the smart card from application As opposed to the access request to said smart card from the application [finishing / finishing / exclusion acquisition of this application / is supposed and / application / exclusion acquisition] The share approach characterized by permitting access to this smart card to the application [finishing / application / this exclusion acquisition] when the application [finishing / application / this exclusion acquisition] is already attested from this smart card.

[0062] (Additional remark 10) The application are the application contain two or more access processings by one smart card, or its library, carry out an exclusion acquisition demand to two or more access processings, respectively at the time of initiation of this access processing, give a discharge notice in exclusion and carry out carrying out an authentication demand to the smart card carry out this access processing only at the time of processing of the beginning of the access processings of said plurality as the description at the time of termination of each access processing, respectively, or its library.

[0063] (Additional remark 11) The library of the application are the library of the application contain two or more access processings by one smart card, carry out an exclusion acquisition demand to two or more access processings, respectively at the time of initiation of this access processing, give a discharge notice in exclusion, respectively

at the time of termination of each access processing, and carry out carrying out an authentication demand to the smart card carry out this access processing only at the time of processing of the beginning of the access processings of said plurality as the description.

[0064] (Additional remark 12) When used by the information processor in which two or more applications carry out juxtaposition actuation, If the logical channel [finishing / a logical channel / exclusion acquisition] exists in this smart card with other applications to the exclusion acquisition demand to the smart card from application As opposed to the access request to said smart card from the application [finishing / finishing / exclusion acquisition of this application / is supposed and / application / exclusion acquisition] When the application [finishing / application / this exclusion acquisition] is already attested from this smart card, The record medium which said information processor which memorized the program to which it makes it carry out to said information processor to permit access to this smart card to the application [finishing / application / this exclusion acquisition] can read.

[0065]

[Effect of the Invention] According to this invention, since exclusive control to a smart card is performed, even if it shares a smart card with two or more applications, authentication of each application unit is enabled.

[0066] Moreover, since authentication processing is performed only when it will be judged whether it is finishing [authentication] and the smart card will not have attested the application if application performs an access request to a smart card since unitary management of the authentication relation between each application and a smart card is carried out, the count of authentication processing can be reduced and the overhead by authentication processing can be made small. Moreover, since authentication processing by PIN is performed only at once first, application does not need to continue holding PIN and can aim at improvement in security level.

[0067] Furthermore, access of a smart card is attained among two or more attested applications, with an authentication condition held. Moreover, application can shorten the waiting state period for exclusion acquisition. Therefore, the parallelism of processing can be improved and compaction of the processing time of each application can be aimed at again.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1] It is drawing showing the configuration at the time of establishing a exclusive control device and performing the exclusive operation of access to a smart card.

[Drawing 2] It is drawing showing the access processing to the smart card of each application at the time of the configuration equipped with the exclusive control device.

[Drawing 3] It is a block diagram at the time of establishing a exclusive control device and an accessor controller.

[Drawing 4] It is drawing showing the example of a configuration of an authentication status management table.

[Drawing 5] It is drawing having shown the flow of processing of the application at the time of application performing access to a smart card, a exclusive control device, and an accessor controller.

[Drawing 6] It is drawing showing the access processing to the smart card of each application at the time of the configuration equipped with the exclusive control device and the accessor controller.

[Drawing 7] It is the flow chart which shows processing of the application which accesses a smart card.

[Drawing 8] It is the flow chart which shows processing of the exclusive control device over the exclusion acquisition demand from application.

[Drawing 9] It is the flow chart which shows processing of the exclusive control device over the notice of discharge of the exclusion from application.

[Drawing 10] It is the flow chart which shows the processing of an accessor controller to the access initiation declaration to the smart card from application.

[Drawing 11] It is the flow chart which shows the processing of an accessor controller to the access request to the smart card from application.

[Drawing 12] It is drawing showing the structure of a system which uses the smart card in this operation gestalt.

[Drawing 13] It is the system environment Fig. of an information processor.

[Drawing 14] It is drawing showing the example of a storage.

[Drawing 15] It is drawing showing the logical construction inside a smart card.

[Description of Notations]

11 Exclusive Control Device

12 Accessor Controller

21 41 Application

22, 42, 59 Smart card

40 Access Control System

43 58 Smart card reader

51 CPU
52 Main Storage
55 Auxiliary Storage Unit
54 I/O Device
55 Network Connection Equipment
56 Medium Reader
57 Portable Storage
60 Bus
71 Information Processor
72 Storage Means
73 Network Circuit
74 Body of Information Processor (Computer)
75 Memory
76 Portable Record Medium

*** NOTICES ***

**JPO and INPI are not responsible for any
damages caused by the use of this translation.**

1. This document has been translated by computer. So the translation may not reflect the original precisely.
2. *** shows the word which can not be translated.
3. In the drawings, any words are not translated.

(19)日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11)特許出願公開番号
特開2002-157554
(P2002-157554A)

(13)公開日 平成14年5月31日 (2002.5.31)

(51)Int.Cl. ⁷	識別記号	F I	チ-コ-1 ⁷ (参考)
G 0 6 K 17/00		G 0 6 K 17/00	E 5 B 0 1 7
G 0 6 F 9/46	3 4 0	G 0 6 F 9/46	3 4 0 F 5 B 0 3 5
12/14	3 1 0	12/14	3 1 0 K 5 B 0 5 8
G 0 6 K 19/073		G 0 6 K 19/00	P 5 B 0 9 8

審査請求 未請求 請求項の数11 O L (全14頁)

(21)出願番号	特願2001-220885(P2001-220885)	(71)出願人	000005223 富士通株式会社 神奈川県川崎市中原区上小田中4丁目1番1号
(22)出願日	平成13年7月23日(2001.7.23)	(72)発明者	栗田 佳 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内
(31)優先権主張番号	特願2000-269096(P2000-269096)	(74)代理人	100074099 弁理士 大曾 義之 (外1名)
(32)優先日	平成12年9月5日(2000.9.5)	Fターム(参考)	5B017 AA07 BA06 CA14 5B035 AA13 CA11 CA29 CA38 5B058 CA23 CA26 KA02 KA04 YA20 5B098 AA03 GA01 GD03 GD15
(33)優先権主張区	日本 (JP)		

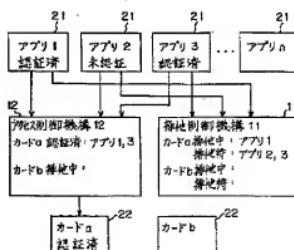
(54)【発明の名前】 スマートカードのアクセス管理システム、共有方法及び記憶媒体

(57)【要約】

【課題】複数のアプリケーションによるアクセスに対し、各アプリケーション(プロセス)毎に認証許可を与えるスマートカードのアクセス管理システム及び管理方法を提供することを課題とする。

【解決手段】スマートカードへの複数のアクセス処理を含むアプリケーション21は、各アクセス処理毎にスマートカード22に対してアクセス要求を行う際、排他制御機器11に対して排他獲得要求を行い、排他が得られるとアクセス制御機器12に対してアクセスを要求する。アクセス制御機器12はアプリケーション21が未認証ならばPINの入力を要求し、既に認証を得られていればスマートカード22へのアクセスを許可する。アプリケーション21はアクセス処理単位で排他獲得要求/解除を行う。

排他制御機構及びアクセス制御機構を
設けた場合の構成図



【特許請求の範囲】

【請求項1】複数のアプリケーションによるスマートカードへのアクセスを管理するスマートカードのアクセス管理システムであって、

アプリケーションからのスマートカードに対する排他獲得要求に対し、該スマートカードに他のアプリケーションによって排他獲得済みとなっていない論理チャネルが存在すれば、該アプリケーションを排他獲得済みとする排他制御手段、

排他獲得済みとなっているアプリケーションからの前記スマートカードへのアクセス要求に対し、該排他獲得済みとなっているアプリケーションが該スマートカードから既に認証されている時、該排他獲得済みとなっているアプリケーションに該スマートカードへのアクセスを許可するアクセス制御手段とを備えることを特徴とするアクセス管理システム。

【請求項2】前記排他制御手段は、アプリケーションからのスマートカードに対する排他獲得要求に対し、該スマートカードに他のアプリケーションによって排他獲得済みとなっていない論理チャネルが存在しなければ、該排他獲得要求を行ったアプリケーションをキューに登録することを特徴とする請求項1に記載のアクセス管理システム。

【請求項3】前記アクセス制御手段は、前記アクセス要求に対し、前記排他を獲得したアプリケーションが前記スマートカードから未認証である時、該アプリケーションの要求を拒否することを特徴とする請求項1又は2に記載のアクセス管理システム。

【請求項4】前記アクセス制御手段は、前記スマートカードがスマートカードリーダーにより抜かれた時、該抜かれたスマートカードにより認証済みとなっているアプリケーションを未認証に変更することを特徴とする請求項1乃至3のいずれか1に記載のアクセス管理システム。

【請求項5】前記アプリケーションは、前記スマートカードに複数回アクセスする時、各アクセスの開始時に前記排他制御手段に前記排他獲得要求を行い、該各アクセスの終了時に前記排他制御手段に排他的解除通知を行うことを特徴とする請求項1乃至4のいずれか1に記載のアクセス管理システム。

【請求項6】前記排他制御手段は、アプリケーションからのスマートカードに対する排他獲得要求に対し、該スマートカードが他のアプリケーションによって既に排他獲得済みであれば、該排他獲得要求を行ったアプリケーションをキューに登録し、前記アプリケーションからの排他的解除通知に対し、前記キューに登録されているアプリケーションを排他獲得済みとすることを特徴とする請求項5に記載のアクセス管理システム。

【請求項7】前記アクセス制御手段は、アプリケーションからスマートカードの認証解除の通知に対し、該認証解除が該スマートカードにより認証済みとなっている

最後のアプリケーションからの時、該スマートカードに認証解除を要求することを特徴とする請求項1乃至6のいずれか1に記載のアクセス管理システム。

【請求項8】複数のアプリケーションによるスマートカードへのアクセスを管理するスマートカードの共有方法であって、

アプリケーションからのスマートカードに対する排他獲得要求に対し、該スマートカードに他のアプリケーションによって排他獲得済みとなっていない論理チャネルが存在すれば、該アプリケーションを排他獲得済みとし、該排他獲得済みとなっているアプリケーションからの前記スマートカードへのアクセス要求に対し、該排他獲得済みとなっているアプリケーションが該スマートカードから既に認証されている時、該排他獲得済みとなっているアプリケーションに該スマートカードへのアクセスを許可することを特徴とする共有方法。

【請求項9】1つのスマートカードへの複数のアクセス処理を含むアプリケーション又はそのライブラリであつて、

複数のアクセス処理に対し、該アクセス処理の開始時にそれぞれ排他獲得要求を行い、各アクセス処理の終了時にそれぞれ排他的解除通知し、前記複数のアクセス処理のうちの最初の処理時のみに該アクセス処理を行うスマートカードに対して認証要求を行ふことを特徴とするアプリケーション又はそのライブラリ。

【請求項10】複数のアプリケーションが並列動作する情報処理装置によって使用された時、

アプリケーションからのスマートカードに対する排他獲得要求に対し、該スマートカードに他のアプリケーションによって排他獲得済みとなっていない論理チャネルが存在すれば、該アプリケーションを排他獲得済みとし、該排他獲得済みとなっているアプリケーションからの前記スマートカードへのアクセス要求に対し、該排他獲得済みとなっているアプリケーションが該スマートカードから既に認証されている時、該排他獲得済みとなっているアプリケーションに該スマートカードへのアクセスを許可することを前記情報処理装置に行わせるプログラムを記憶した前記情報処理装置が読み出し可能な記録媒体。

【請求項11】複数のアプリケーションが並列動作する情報処理装置によって実行された時、

アプリケーションからのスマートカードに対する排他獲得要求に対し、該スマートカードに他のアプリケーションによって排他獲得済みとなっていない論理チャネルが存在すれば、該アプリケーションを排他獲得済みとし、該排他獲得済みとなっているアプリケーションからの前記スマートカードへのアクセス要求に対し、該排他獲得済みとなっているアプリケーションが該スマートカードから既に認証されている時、該排他獲得済みとなっているアプリケーションに該スマートカードへのアクセスを許可することを前記情報処理装置に行わせるプログラムを記憶した前記情報処理装置が読み出し可能な記録媒体。

可することを前記情報処理装置に行わせるプログラム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、スマートカード上のデータの複数プロセスによる共有した場合のスマートカードのアクセス管理に関する。

【0002】

【従来の技術】スマートカードは、従来用いられている磁気カードに比して非常に大きな容量のデータを記憶することが出来るなどから、様々な分野への使用が検討され、あるいは実用化されている。

【0003】またスマートカードは、内部にメモリと共にCPUを備えており、このCPUを介してメモリ内のデータへアクセスを行うので、アクセス時にCPUに認証処理を行わせることにより、従来の磁気カードに比べて高いセキュリティ性を実現出来、この点もスマートカードのメリットとなっている。

【0004】スマートカードはPIN(Personal Identification Number)によるセキュリティ機能を持っており、この機能によりPINの組合を行い、認証された場合にだけカード内の秘密情報をアクセスすることができるよう前衛することが可能である。このPINによる認証は、いわゆるパスワード入力方式で、スマートカードを用いるユーザがPINとして例えばパスワードを入力し、これをスマートカード内に記憶しているパスワードとカード内で比較して、一致した場合に内部データへのアクセスを許可する。

【0005】スマートカードへのアクセスは、スマートカードが持つ論理チャネルを通して行い、認証要求は論理チャネルに対して行われる。そしてスマートカードは、この論理チャネル毎にPINによる認証状態などをセキュリティに関する状態を保持している。

【0006】図15は、アプリケーションから見たスマートカード内部の論理的構成を示したものである。スマートカード内では、データをツリーフォーマットの構成によって管理しており、最上位にあるDIRの下層に、使用されるアプリケーション毎の単位等でDF(Delicated File)が設けられている。そして、各DF内には実際のデータを保持しているEF(Elementary File)が格納されている。スマートカードからデータにアクセスする際、アプリケーションは、まずアクセスを行うデータの位置を示す位番情報を送って、目的のEFにアクセス位置を移動した後、そのEFからデータの読みだし/書き込みを行う。また各チャネルは、現在のアクセス位置を状態情報として保持している。

【0007】

【発明が解決しようとする課題】現在スマートカードを複数のアプリケーションで同時に使用する使い方が検討されている。例えば公開鍵暗号方式をベースとしたPKI(Public Key Infrastructure)システムを構築し、この

システム上のコンピュータで複数のアプリケーションが稼働している場合に、各アプリケーションがデジタル署名などによるセキュリティ認証にスマートカードを用いることが、現在スマートカードの1つの使用方法として考えられている。

【0008】この場合、スマートカードを接続したコンピュータ上の複数のアプリケーションがスマートカードを共用することになる。そして1つのスマートカードが持つ論理チャネルの数はせいぜい2チャネル程度なので、多数のアプリケーションに同一のカードに対してアクセスさせる場合、1つの論理チャネルを複数のアプリケーションが共有する必要が出てくる。尚本明細書内の以下の説明は、説明の簡略化のため、1つのアプリケーションは1つのプロセスで構成されることを前提としており、アプリケーションという言葉をプロセスと同義で用いている。通常1つのアプリケーションは1つのプロセスで構成されることが多いが、複数のプロセスで構成されている場合でも、アプリケーションをプロセスと置換えて考えれば、以下の説明は基本的に同じである。

【0009】現行のスマートカードのセキュリティ方式では、1つのアプリケーションがある論理チャネルに対してPIN認証を行い、アクセス許可を得ると、以降その論理チャネルからは、認証が解除されるまでの間、認証を受けたアプリケーションだけでなく他のアプリケーションもアクセス出来てしまう。

【0010】複数のアプリケーションで1つのカードの同じ機能を共有することを、セキュリティの観点から考えると、個々のアプリケーション毎にPINによる認証を行った方がセキュリティレベルはより強固になる。しかし、現行のスマートカードへのアクセス制御では、1つの論理チャネルを複数のアプリケーションで共有する場合、論理チャネル毎に認証が行われる各論理チャネルに認証状態(アクセス許可を与えたか否か)が保持されるため、1つのアプリケーションがPINによる認証を行ってアクセス許可を得れば、他のアプリケーションはPINによる認証を受けずに、その論理チャネルからカードへのアクセスが可能となってしまう。

【0011】また、上述したように各アプリケーションは、カード内のデータにアクセスする際、位置付け情報と論理チャネルに連携してアクセス位置を移動してからデータの書き込み/読みだしを行うが、複数のアプリケーションが論理チャネルを共有する場合、各アプリケーションはカレントのアクセス位置の把握が難しくなる。

【0012】上記問題点を鑑み、本発明は、複数のアプリケーション(プロセス)によるアクセスに対し、スマートカードへの認証状態を一元管理することにより、各アプリケーション(プロセス)毎に認証許可を与えるスマートカードのアクセス管理システム及び管理方法を提供することを課題とする。また、各アプリケーション(プロセス)毎の認証を認証処理によるオーバヘッドを

大きくすること無く実現するアクセス管理システム及び管理方法を提供することを課題とする。

【0013】

【課題を解決するための手段】上記問題点を解決するため、本発明によるスマートカードのアクセス管理システムは、複数のアプリケーションによるスマートカードへのアクセスを管理するものであって、排他制御手段及びアクセス制御手段を備える。

【0014】排他制御手段は、アプリケーションからのスマートカードに対する排他獲得要求に対し、該スマートカードに他のアプリケーションによって排他獲得済みとなっていない論理チャネルが存在すれば、該アプリケーションを排他獲得済みとする。また上記排他制御手段は、アプリケーションからのスマートカードに対する排他獲得要求に対し、該スマートカードに他のアプリケーションによって排他獲得済みとなっていない論理チャネルが存在しなければ、該排他獲得要求を行ったアプリケーションをキーに登録する。

【0015】アクセス制御手段は、排他獲得済みとなっているアプリケーションからの上記スマートカードへのアクセス要求に対し、該排他獲得済みとなっているアプリケーションが該スマートカードから既に認証されている時、該排他獲得済みとなっているアプリケーションに該スマートカードへのアクセスを許可する。またアクセス制御手段は、上記アクセス要求に対し、上記排他を獲得したアプリケーションが上記スマートカードから未認証である時、該アプリケーションにPINの入力を要求する。各アプリケーションによるスマートカードの認証はこのアクセス制御手段を通して行われ、アクセス制御手段は各アプリケーションとスマートカードとの認証関係を把握している。

【0016】本発明によれば、排他制御手段により、スマートカードに対する排他制御が行われるので、複数のアプリケーションによってスマートカードを共用しても各アプリケーション毎の認証を可能とする。

【0017】また、アクセス制御手段により、各アクセス要求を行ったアプリケーションが認証済みかどうかが判断され、認証済みの場合、認証処理を行わずにアクセス許可を与えるので、認証処理回数を削減することが出来る。

【0018】

【発明の実施の形態】以下に本発明の一実施形態について、図面を参照しながら説明する。各アプリケーション毎に認証許可を与えるようにするために、スマートカード（スマートカードが複数の論理チャネルをもつ場合論理チャネル）に対して排他制御を行い、認証された1つのアプリケーションがスマートカードを使用している間、そのアプリケーションがカード（若しくは論理チャネル）を專有し、他のアプリケーションからのアクセスを抑制する必要がある。尚説明簡略化の為、以下の実施

形態では各スマートカードは論理チャネルを1つ備える構成とする。尚スマートカードが複数論理チャネルを備えた場合は、以下に説明する排他制御は論理チャネル単位で行われる。

【0019】図1は、排他制御機構を設け、スマートカードにアクセスするアプリケーションの排他処理を行った場合を示す。図1では、複数のアプリケーション21とスマートカード22の間に排他制御機構11を設け、スマートカード22に対してアクセスを要求する際、各アプリケーション21はこの排他制御機構11に対して排他獲得要求を行い、排他が得られたアプリケーション21が、スマートカード22を専有してアクセスを行う。同図の排他制御機構11はカードa、bの2つのカードへのアクセスに対する排他を審理している。そしてアプリ1、アプリ2及びアプリ3の3つのアプリケーション21がカードaに対してアクセス要求を発行しており、排他制御機構11はそのうちのアプリ1に対して排他獲得し、他のアプリ2及び3はカードaが解放されるまで待ち状態にしておく。排他が獲得したアプリ1は、カードaの論理チャネルに対してPIN認証を行った後データの読みだし/書き込みを行う。この間他のアプリケーション21は、カードaに対してアクセスすることが出来ない。アプリ1の処理を完了してカードaを解放すると、次に、待ち状態となっているアプリ2が排他を獲得し、カードaに対してPIN認証を行った後内部のデータにアクセスする。この様に排他制御機構11を設けることにより、認証を受けた1つのアプリケーションのスマートカードに対してアクセスすることが出来、各アプリケーション21毎の認証を実現することが出来る。

【0020】この図1の構成による方式の場合、1つのアプリケーション21がスマートカード22を使用している間このスマートカード22はこのアプリケーション21に専有されるので、他のアプリケーション21は排他が解除されスマートカード22が解放されるまで待ち状態になる。よってこの方式では、複数のアプリケーションの並列処理性能が悪く、また待ち状態にあるアプリケーションは長い期間処理を停止してハングアップした状態に見える等、非常に使い勝手が悪くなる。

【0021】これを回避するものとしては、アプリケーション21がスマートカード22へのアクセス処理が完了すると専有していたスマートカード22を逐一開放する方式がある。この方式では、アプリケーション21が複数回スマートカード22に対するアクセス処理を含む場合、各アクセス処理毎に排他制御機構11に対してスマートカード22への排他獲得/開放を行い、こまめに排他制御を区切る。

【0022】図2に、この方式による各アプリケーションのスマートカードの排他獲得/開放の例を示す。同図は、図1と同様アプリ1、アプリ2及びアプリ3の3

7
つのアプリケーション21がカードaに対してアクセス要求を発行した場合の各アプリケーションのスマートカードへのアクセス処理を示すもので、同図中排他制御機構11への矢印1は、各アプリケーション21から排他制御機構11への排他獲得要求、排他制御機構11からの矢印1は排他制御機構11から各アプリケーション21への排他獲得の通知を示す。また斜線部分は各アプリケーション21によるPIN認証処理、網掛け部分はスマートカード22へのアクセス処理を示す。

【0023】排他を獲得したアプリケーション21が、全処理が完了するまで排他を解除してスマートカード22を解放しなかった場合、アプリ2は排他制御機構11にカードaへの排他獲得要求を行った図2中の31の位置から、既にカードaへの排他を獲得しているアプリ1が処理が完了する33の位置まで、更にアプリ3は32の位置からこのアプリ2の処理が完了するまで待ち状態となる。しかし、同図の様にアプリケーション21が各アクセス処理毎にこまめに排他制御を区切ることにより、排他が解除された期間間に他のアプリケーション21がカードaにアクセスすることが出来るので、排他獲得の為の待ち状態となり処理が停止してしまう期間が短くなり、処理の並列性が向上する。

【0024】この様に、排他制御を頻繁に切替えると、各アプリケーションの待ち状態の期間は短くなり処理の並列性は向上する。しかし図2の斜線部に示すように各アプリケーションは切替えの度に認証状態の設定/解除処理を行う必要があり、その為のオーバヘッドが大きくなってしまう。また認証の再許可を得る際PINを送信するので、各アプリケーション21がPINを保持し続けることになり、セキュリティ上の問題も生じる。これを回避するため、認証処理の度にユーザがパスワードを入力する構成とすると共に認証処理のオーバヘッドが大きくなる。

【0025】図3にこの点を考慮した構成を示す。図3の構成では、複数のアプリケーション21とスマートカード22の間に、排他制御機構11に加えアクセス制御機構12を設け、このアクセス制御機構12によって各アプリケーション21のスマートカード22による認証を一元管理しながら、排他制御機構11がスマートカード22にアクセスするアプリケーション21の排他処理を行っている。

【0026】各アプリケーション21はスマートカード22に対してアクセスを要求する際、まず排他制御機構11に対して排他獲得要求を行い、排他が獲得できることにアクセス制御機構12にスマートカード22への認証を依頼する。そして認証が得られるとスマートカード22内のデータにアクセスする。

【0027】アクセス制御機構12は認証状態管理テーブルを持ち、この認証状態管理テーブルを用いてアプリケーション21がスマートカード22への認証の開始宣

言を行ってから認証の解除を通知するまでの間にについて各アプリケーションとスマートカード22との認証状態の管理を行う。

【0028】図4は、認証状態管理テーブルの構成例を示す図である。認証状態管理テーブルは、各アプリケーション21が現在どのスマートカード22から認証を得ているのかを排他制御機構11が管理するために用いるテーブルで、アプリ識別情報と認証済みカード情報に対応づけて記憶している。アプリ識別情報は、各アプリケーション21を識別するための一意な識別子を記憶するもので、この識別子は、一般的なアプリケーションが操作できないものが用いられ、例えばプロセス生成時に各プロセスに付加され、カーネルが管理しているプロセスIDを用いる。あるいは、スマートカードへのアクセスへのアクセス要求を行ったアプリケーション21に対してアクセス制御機構12が識別子を順次生成付加してゆく構成としてもよい。

【0029】図4はカードa、bの2つのスマートカード22に対する各アプリケーション21の認証状態を管理する場合を例示しており、各アプリケーションに対し認証済みカード情報としてそのアプリケーション21が認証しているカードが記録されている。尚認証済みカード情報が空欄の部分は、そのアプリケーションに対し認証済みとなっているスマートカードが存在しないことを示す。同図では、アプリ1はカードa、b両方が認証済み、アプリ2、アプリ3はいずれも未認証、アプリ3はカードaのみ認証済みとなっている。

【0030】各アプリケーション21は、スマートカード22に対する認証及びスマートカード22へのアクセスをアクセス制御機構12を介して行う。アプリケーション21からスマートカード22へのアクセス要求が有る際、認証状態管理テーブルを参照してそのアプリケーション21がアクセス要求したスマートカード22に認証済みであるかどうかを調べ、未認証ならばアプリケーション21からの要求を拒絶し、またアプリケーション21にPINの入力を要求してスマートカード22との認証処理を行う。また、そのアプリケーション21が認証済みならばアプリケーション21は既にそのスマートカード21の認証許可を得ているのでスマートカード21へのアクセスを許可し、実行する。

【0031】図5はアプリケーション21がスマートカード22へのアクセスを行う際の、アプリケーション21、排他制御機構11及びアクセス制御機構12の処理の流れを示した図である。同図はアプリ1がカードaに対してアクセスを行う場合を例としており、また以下の説明中の1)～23)は図5中の番号に対応している。

1) アプリ1はカードaへの排他開始を行うため、排他制御機構11に対し、排他獲得要求を行う。
2) アプリ1からの要求に対し、排他制御機構11は、カードaに対し排他獲得済のアプリケーションが有るか

調べ、既に他のアプリケーションが獲得していたならば排他待ちのキューに登録する。また排他獲得済でなければ、アプリ1に排他獲得を通知する。

3) アプリ1は、アクセス制御機構12にカードaへのアクセス開始宣言を行う。

4) アクセス開始宣言に対しアクセス制御機構12は、認証状態管理テーブルにアプリ1を登録する。そして、アプリ1にPINの入力要求を行う。尚アプリ1がカードbにもアクセス開始宣言を行っている場合は、アプリ1は既に認証状態管理テーブルに登録してあるのでカードaに対するアクセス開始宣言で再度認証状態管理テーブルに登録する必要はない。

5) アプリ1はユーザにパスワードの入力を促し、ユーザの入力からPINを指定してカードaへの認証を要求する。

6) 排他制御機構11は、カードaに対しPINを通知し、カードaに認証チェックを行わせる。

7) アクセス制御機構12は、カードaによる認証チェックの結果、認証が得られれば、認証状態管理テーブルにアプリ1がカードaに認証済みであることを登録する。

8) アプリ1はアクセス制御機構12に対し、カードaへのデータの読み出し/書き込みを要求する。

9) アプリ1からの読み出し/書き込み要求に対し、認証状態管理テーブルを検索し、アプリ1が認証済カードaに認証済みならばカードaに対してアクセスを行。未認証ならば、アプリ1にエラーを通知する。

10) 1つのアクセス処理が完了しカードaの専有を解除する場合に、アプリ1は排他制御機構11に排他の解除を通知する。

11) 排他制御機構11は、登録されているアプリ1のカードaに対する排他獲得を削除し、他のカードaへの排他待ちのキューに登録されているアプリケーション21があればそのアプリケーション21の排他獲得を登録する。

12) 排他の解除後、アプリ1はカードaへのアクセス処理以外の処理を行う。この間、カードaの排他を解放しているので他のアプリケーション21がカードaを使用することが出来る。

13) アプリ1は、再度カードaへのアクセスの必要が生じると、排他制御機構11に排他獲得要求を行う。

14) アプリ1からの要求に対し、排他制御機構11は2)と同様、カードaに対し排他獲得済のアプリケーションが有るか再度調べ、既に他のアプリケーションが排他獲得済でなければ、アプリ1に排他獲得を通知する。

15) アプリ1はアクセス制御機構12に対し、カードaへのデータの読み出し/書き込みを要求する。

16) アクセス制御機構12は、再度9)と同様な処理を行。この時7)で、認証状態管理テーブルにアプリ

1がカードaに認証済みであることが登録されているの

で、そのままカードaへアクセスを行う。以降アプリ1内のカードaへのアクセス処理の回数分10)~1~6)の処理が繰り返される。

17) 全アクセス処理が完了するとアプリ1は、アクセス制御機構12にカードaへの認証を解除を通知する。

18) アクセス制御機構12は、認証状態管理テーブルのアプリ1からカードa認証済の情報を削除する。

19) アクセス制御機構12は、認証状態管理テーブル13に他のカードaに認証されているアプリケーション

10) 21が存在しなくなるまで認証状態を保持し、認証されているアプリケーション21が存在しなくなるとカードaに認証解除を要求する。これにより同一のスマートカードとの認証処理の回数を削減することが出来る。

20) アプリ1は、アクセス制御機構12にスマートカード22へのアクセス終了を通知する。

21) 20)での通知を受けるとアクセス制御機構12は認証状態管理テーブルから、アプリ1を削除する。この時アプリ1が他のスマートカード22に対してはまだアクセスを終していない場合は認証状態管理テーブルからアプリ1を削除しない。

22) アプリ1は排他制御機構11にカードaの排他の解除を通知する。

23) 排他制御機構11は、再度11)と同様な処理を行、排他を解除する。

【0032】図6は、図3の排他制御機構11及びアクセス制御機構12を構成する各アプリケーションのスマートカードへの処理を示す図である。同図は、比較のため図2と同じ前述の元での同じアプリケーション21の処理を示してある。図6を図2と比較すると、

30) 各アプリケーション21は、認証処理としては、一番最初のカードaへのアクセス処理開始時のPINによる認証処理と、一番最後のアクセス処理終了時にカードaへの認証の解除処理を行っているのみで、図2では行っていたカードaへの各アクセス処理毎の認証処理が省略されている。よって各アプリケーション21は認証処理が省略された分処理時間が短くなる。また各アプリケーション21が、カードaを専有している期間も認証処理が省略された分だけ短くなるので、その分待ち状態となる期間が短くてすむ可能性がある。更に各アプリケーション21は、スマートカード22に対するPIN認証を最初に1度だけ行えばよいので、カードから認証が得られればPINを破棄することが出来る。

【0033】図7は、本システムによりスマートカード22にアクセスを行うアプリケーション21の処理を示すフローチャートである。尚これらの処理を行う機構をアプリケーション21に直接持たせる構成とすることも出来るが、これらの処理をライブラリとして実現し、このライブラリを各アプリケーション21に組み込む形態を取るのが一般的な構成である。

【0034】アプリケーション21は、スマートカード

2 2 にアクセスを行ふ際、まず排他制御機器 1 1 へ排他獲得の依頼を行い (ステップ S 1) 、排他制御機器 1 1 からの応答を待つ。その結果、排他制御機器 1 1 から何等かの理由で、排他が獲得出来ない旨の通知が有れば (ステップ S 2、NO) 、処理を終了する。

【0035】排他獲得の依頼に対し、排他制御機器 1 1 から排他獲得成功の通知が有れば (ステップ S 2、YES) 、次にステップ S 3 として、アクセス制御機器 1 2 にスマートカード 2 2 へのアクセスの開始宣言を行う。

【0036】このスマートカード 2 2 へのアクセスが未認証のスマートカード 2 2 へのアクセスであり、スマートカード 2 2 への認証が必要なためアクセス制御機器 1 2 から PIN の入力を要求された時 (ステップ S 4、YES) 、ステップ S 8 として PIN としてユーザーが入力したパスワードをアクセス制御機器 1 2 に送って、認証処理を依頼し確認を行う。その結果認証されれば (ステップ S 9、YES) 、処理をステップ S 5 に移してスマートカードへアクセスし、認証されなければ (ステップ S 9、NO) 、処理を終了する。

【0037】ステップ S 4 において、このアクセスが既に認証を得ているスマートカード 2 2 へのアクセスである時 (ステップ S 4、NO) 、更なる認証処理は必要無いので、ステップ S 5 としてスマートカード 2 2 へのアクセスを許可してデータの読み出し/書き込みを行う。

【0038】ステップ S 5 のアクセス処理が終了すると、ステップ S 6 として、アクセス制御機器 1 2 に対しでスマートカード 2 2 へのアクセスの終了宣言を行う。そしてステップ S 7 として、そのスマートカード 2 2 への排他の解除を排他制御機器 1 1 に通知してスマートカード 2 2 へのアクセス処理を終了する。

【0039】図 8 は、アプリケーション 2 1 からの排他獲得要求に対する排他制御機器 1 1 の処理を示すフローチャートである。アプリケーション 2 1 から、スマートカード 2 2 への排他獲得要求があると、排他制御機器 1 1 は、ステップ S 1 として、排他獲得を要求されたスマートカード 2 2 が、既に他のアプリケーション 2 1 によって排他獲得済みであるかどうかを判断する。その結果他のアプリケーション 2 1 による排他獲得が行われていなければ (ステップ S 1 1、NO) 、そのスマートカード 2 2 を排他獲得済みとして登録し、要求を行ったアプリケーション 2 2 に排他獲得を通知して処理を終了する。

【0040】またステップ S 1 1 で他のアプリケーション 2 1 が排他獲得済みであるならば (ステップ S 1 1、YES) 、ステップ S 1 2 としてこの排他獲得要求を排他待ちキューに追加して処理を終了する。

【0041】図 9 は、アプリケーション 2 1 からの排他の解除通知に対する排他制御機器 1 1 の処理を示すフローチャートである。アプリケーション 2 1 からスマートカード 2 2 への排他の解除通知を受けると、排他制御機

機 1 1 は、ステップ S 2 1 としてそのアプリケーション 2 1 の排他獲得済みの登録を削除して排他を解除する。

【0042】そして排他待ちキューを調べ、排他が解除されたスマートカード 2 2 に対して排他待ちとなっているアプリケーション 2 1 が存在すれば (ステップ S 2 2、YES) 、排他待ちキューの先頭に登録されているアプリケーション 2 1 のスマートカード 2 2 への排他獲得を登録してスマートカード 2 2 をディスパッチした後、また排他待ちキューに待ちが存在しなければ (ステップ S 2 2、NO) そのまま、処理を終了する。

【0043】図 10 は、アプリケーション 2 1 からのスマートカード 2 2 へのアクセス要求に対するアクセス制御機器 1 2 の処理を示すフローチャートである。アプリケーション 2 1 からのアクセス開始宣言に対し、アクセス制御機器 1 2 は、ステップ S 3 1 として、認証状態管理テーブルにアプリケーション 2 1 を登録して、スマートカード 2 2 に対してアクセス要求プロセスを登録する。

【0044】図 11 は、アプリケーション 2 1 からのスマートカード 2 2 へのアクセス要求に対するアクセス制御機器 1 2 の処理を示すフローチャートである。アプリケーション 2 1 からのアクセス要求に対し、アクセス制御機器 1 2 はステップ S 4 1 として認証状態管理テーブルを参照して、そのアプリケーション 2 1 がアクセス要求先のスマートカード 2 2 から既に認証済であるかどうかを調べる。その結果、既に認証済みであれば (ステップ S 4 1、YES) 、更なる認証は必要無いので、ステップ S 4 5 としてアプリケーション 2 1 に対してアクセス許可を通知する。

【0045】ステップ S 4 1 で、そのアプリケーション 2 1 がまだ認証を得ていないのならば (ステップ S 4 1、NO) 、認証処理を行う必要があるので、ステップ S 4 2 としてアプリケーション 2 1 にパスワードの入力を要求し、スマートカード 2 2 に対して PIN による認証チェックを依頼する。その結果、スマートカード 2 2 から認証が得られれば、ステップ S 4 5 としてアプリケーション 2 1 に対してアクセス許可を通知し、また認証が得られなければ (ステップ S 4 3、NO) 、アクセス不許可をアプリケーション 2 1 に対して通知して処理を終了する。

【0046】図 12 は、本実施形態に於けるスマートカードを使用するシステムの構成を示す図である。本実施形態でのアプリケーション 4 1 とスマートカード 4 2 との間を管理するアクセス管理システム 4 0 は、スマートカードリーダ 4 3 と各アプリケーション 4 1 のライブラリ 4 4 との間に構成され、OS の一機能として、あるいは OS に実装される形で実現される。

【0047】アプリケーション 4 1 は、スマートカード 4 2 に対する認証処理やアクセス処理を、全てこのアクセス管理システム 4 0 を介して行い、アクセス管理シス

テム40は、各アプリケーション41とスマートカード42との間のやり取りを把握している。またアクセス管理システム40は、スマートカードリーダ43の状態も把握しており、例えばスマートカードリーダ43からスマートカード42が抜かれる等、認証状態管理テーブルを調べ、そのカードが認証済みとしているアプリケーションが何が未認証に変更する。

【0048】なお、アクセス管理システム40は、内部に排他制御機能11とアクセス制御機能12を別々に持つ構成となっているが、これらを1つの機能構成要素として実現することもある。また、セキュリティ上、アクセス制御機能や排他制御機能は、複数のアプリケーションが共有できる必要があるので、OSのカーネル内に実現するとセキュリティをより向上することができる。

【0049】図13は、本実施形態における上記スマートカードのアクセス管理をコンピュータプログラムにより実現した場合の情報処理装置システム環境図である。スマートカードを実装した情報処理装置は、図13の様にCPU51、ROM、RAMによる主記憶装置52、補助記憶装置53、ディスプレイ、キーボード等の入出力装置(1/O)54、LANやWAN、一般回線等により他の情報処理装置とネットワーク接続を行うモジュール等のネットワーク接続装置55、ディスク、磁気テープなどの可搬記録媒体57から記憶内容を読み出す媒体読み取り装置56及び1乃至複数のスマートカード59を有し、これらが互いにバス60により接続される構成を備えている。

【0050】また図13の情報処理システムでは、媒体読み取り装置56により磁気テープ、フロッピーディスク等の記録媒体57を用いてアプリケーションソフトの交換が行われる場合がある。よって、本発明は、スマートカードのアクセス管理システムと共有方法に限らず、コンピュータにより使用されたときに、上述の本発明の実施の形態の機能をコンピュータに行わせるためのコンピュータ読み出し可能な記録媒体57として構成することもできる。

【0051】また、この情報処理装置では、フロッピーディスク等の記録媒体57を用いてアプリケーションソフトの交換が行われる場合がある。よって、本発明は、スマートカードのアクセス管理システムと共有方法に限らず、コンピュータにより使用されたときに、上述の本発明の実施の形態の機能をコンピュータに行わせるためのコンピュータ読み出し可能な記録媒体57として構成することもできる。

【0052】この場合、「記録媒体」には、例えば図14に示されるように、CD-ROM、フロッピーディスク(あるいはMO、DVD、リムーバブルハードディスク等であってもよい)等の媒体駆動装置77に説明可能な可搬記録媒体67や、ネットワーク回線73経由で送信される外部の装置(サーバ等)内の記憶手段(データ

ベース等)72、あるいは情報処理装置71の本体74内のメモリ(RAM又はハードディスク等)75等が含まれる。可搬記録媒体67や記憶手段(データベース等)72に記憶されているプログラムは、本体74内のメモリ(RAM又はハードディスク等)75にロードされて、実行される。

【0053】(付記1) 複数のアプリケーションによるスマートカードへのアクセスを管理するスマートカードのアクセス管理システムであって、アプリケーションからのスマートカードに対する排他獲得要求に対し、該スマートカードに他のアプリケーションによって排他獲得済みとなっていない論理チャネルが存在すれば、該アプリケーションを排他獲得済みとする排他制御手段と、該排他獲得済みとなっているアプリケーションからの前記スマートカードへのアクセスに対し、該排他獲得済みとなっていないアプリケーションが該スマートカードから既に認証されている時、該排他獲得済みとなっているアプリケーションに該スマートカードへのアクセスを許可するアクセス制御手段を備えることを特徴とするアプリケーションシステム。

【0054】(付記2) 前記排他制御手段は、アプリケーションからのスマートカードに対する排他獲得要求に対し、該スマートカードに他のアプリケーションによって排他獲得済みとなっていない論理チャネルが存在しなければ、該排他獲得要求を行ったアプリケーションをキューに登録することを特徴とする付記1に記載のアクセス管理システム。

【0055】(付記3) 前記アクセス制御手段は、前記アクセス要求に対し、前記排他を獲得したアプリケーションが前記スマートカードから未認証である時、該アプリケーションの要求を拒絶することを特徴とする付記1又は2に記載のアクセス管理システム。

【0056】(付記4) 前記アクセス制御手段は、アプリケーションとスマートカードとの認証関係を該アプリケーションのプロセスIDを用いて管理することを特徴とする付記1乃至3のいずれか1に記載のアクセス管理システム。

【0057】(付記5) 前記アクセス制御手段は、前記スマートカードがスマートカードリーダより抜かれた時、該抜かれたスマートカードにより認証済みとなっていないアプリケーションを未認証に変更することを特徴とする付記1乃至4のいずれか1に記載のアクセス管理システム。

【0058】(付記6) 前記アプリケーションは、前記スマートカードに複数回アクセスする時、各アクセスの開始時に前記排他制御手段に前記排他獲得要求を行い、該各アクセスの終了時に前記排他制御手段に排他的解除通知を行うことを特徴とする付記1乃至5のいずれか1に記載のアクセス管理システム。

【0059】(付記7) 前記排他制御手段は、アプリ

40

50

ケーションからのスマートカードに対する排他獲得要求に対し、該スマートカードが他のアプリケーションによって既に排他獲得済みであれば、該排他獲得要求を行ったアプリケーションをキューに登録し、前記アプリケーションからの排他の解除通知に対し、前記キューに登録されているアプリケーションを排他獲得済みとすることを特徴とする付記6に記載のアクセス管理システム。

【0060】(付記8) 前記アクセス制御手段は、アプリケーションからスマートカードの認証解除の通知に対し、該認証解除が該スマートカードにより認証済みとなっている最後のアプリケーションからの時、該スマートカードに認証解除を要求することを特徴とする付記1乃至7のいずれか1に記載のアクセス管理システム。

【0061】(付記9) 様数のアプリケーションによるスマートカードへのアクセスを管理するスマートカードの共有方法であって、アプリケーションからのスマートカードに対する排他獲得要求に対し、該スマートカードに他のアプリケーションによって排他獲得済みとなっていない論理チャネルが存在すれば、該アプリケーションを排他獲得済みとし、排他獲得済みとなっているアプリケーションからの前記スマートカードへのアクセスを許可することを特徴とする共有方法。

【0062】(付記10) 1つのスマートカードへの複数のアクセス処理を含むアプリケーション又はそのライブラリであって、複数のアクセス処理に対し、該アクセス処理の開始時にそれぞれ排他獲得要求を行い、各アクセス処理の終了時にそれぞれ排他の解除通知し、前記複数のアクセス処理のうちの最初の処理時のみに該アクセス処理を行なうスマートカードに対して認証要求を行なうことを特徴とするアプリケーション又はそのライブラリ。

【0063】(付記11) 1つスマートカードへの複数のアクセス処理を含むアプリケーションのライブラリであって、複数のアクセス処理に対し、該アクセス処理の開始時にそれぞれ排他獲得要求を行い、各アクセス処理の終了時にそれぞれ排他の解除通知し、前記複数のアクセス処理のうちの最初の処理時のみに該アクセス処理を行なうスマートカードに対して認証要求を行なうことを特徴とするアプリケーションのライブラリ。

【0064】(付記12) 様数のアプリケーションが並列動作する情報処理装置によって使用された時、アプリケーションからのスマートカードに対する排他獲得要求に対し、該スマートカードに他のアプリケーションによって排他獲得済みとなっていない論理チャネルが存在すれば、該アプリケーションを排他獲得済みとし、排他獲得済みとなっているアプリケーションからの前記スマ

ートカードへのアクセス要求に対し、該排他獲得済みとなっているアプリケーションが該スマートカードから既に認証されている時、該排他獲得済みとなっているアプリケーションに該スマートカードへのアクセスを許可することを前記情報処理装置に行わせるプログラムを記憶した前記情報処理装置が読み出し可能な記録媒体。

【0065】

【発明の効果】本発明によれば、スマートカードに対する排他制御が行われるので、複数のアプリケーションによってスマートカードを共用しても各アプリケーション単位の認証を可能とする。

【0066】また、各アプリケーションとスマートカードとの間の認証関係が一元管理されているので、アプリケーションがスマートカードにアクセス要求を行うとそのスマートカードはそのアプリケーションを認証済みかどうかが判断され、未認証の場合のみ認証処理が行われるので、認証処理回数を削減することが出来、認証処理によるオーバヘッドを小さくすることが出来る。またPINによる認証処理は、最初に一度だけ行われるのでアプリケーションは、PINを保持し続ける必要がなく、セキュリティレベルの向上が図れる。

【0067】更にスマートカードは、認証状態を保持したまま複数の認証済みアプリケーションとの間でアクセスが可能となる。またアプリケーションは、排他獲得の為の待ち状態時間を短く出来る。よって処理の並列性を向上出来た各アプリケーションの処理時間の短縮を図れる。

【画面の簡単な説明】

【図1】排他制御機構を設け、スマートカードへのアクセスの排他処理を行なった場合の構成を示す図である。

【図2】排他制御機構を備えた構成時の各アプリケーションのスマートカードへのアクセス処理を示す図である。

【図3】排他制御機構及びアクセス制御機構を設けた場合の構成図である。

【図4】認証状態管理テーブルの構成例を示す図である。

【図5】アプリケーションがスマートカードへのアクセスを行なう際の、アプリケーション、排他制御機構及びアクセス制御機構の処理の流れを示した図である。

【図6】排他制御機構及びアクセス制御機構を備えた構成時の各アプリケーションのスマートカードへのアクセス処理を示す図である。

【図7】スマートカードにアクセスを行なうアプリケーションの処理を示すフローチャートである。

【図8】アプリケーションからの排他獲得要求に対する排他制御機構の処理を示すフローチャートである。

【図9】アプリケーションからの排他の解除通知に対する排他制御機構の処理を示すフローチャートである。

【図10】アプリケーションからのスマートカードへの

アクセス開始宣言に対するアクセス制御機構の処理を示すフローチャートである。

【図1 1】アプリケーションからのスマートカードへのアクセス要求に対するアクセス制御機構の処理を示すフローチャートである。

【図1 2】本実形態に於けるスマートカードを使用するシステムの構成を示す図である。

【図1 3】情報処理装置のシステム環境図である。

【図1 4】記憶媒体の例を示す図である。

【図1 5】スマートカード内部の論理的構成を示す図である。

【符号の説明】

1 1 排他制御機構

1 2 アクセス制御機構

2 1 、 4 1 アプリケーション

2 2 、 4 2 、 5 9 スマートカード

* 4 0 アクセス管理システム

4 3 、 5 8 スマートカードリーダ

5 1 C P U

5 2 主記憶装置

5 5 助記憶装置

5 4 入出力装置

5 5 ネットワーク接続装置

5 6 媒体読み取り装置

5 7 可搬記憶媒体

6 0 バス

7 1 情報処理装置

7 2 記憶手段

7 3 ネットワーク回線

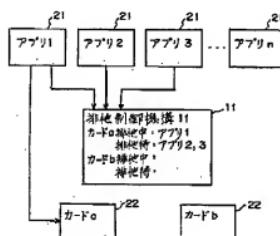
7 4 情報処理装置本体（コンピュータ）

7 5 メモリ

* 7 6 可搬記憶媒体

【図1】

排他制御機構を設け、スマートカードへの
アクセスの排他処理を行った場合の構成
を示す図



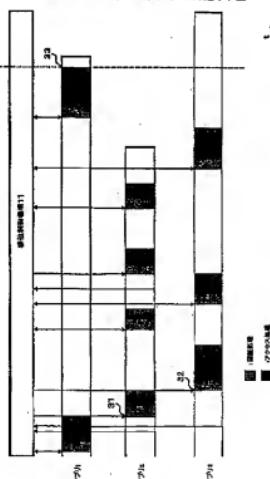
【図2】

認証状態管理テーブルの
構成例を示す図

アクリ種別情報	認証済みカード情報
アクリ1	カードa
アクリ2	カードb
アクリ3	カードa
.....
アクリn	

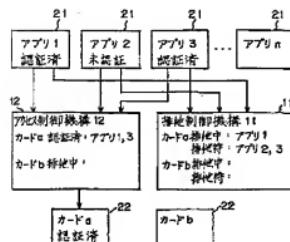
【図2】

排他制御機構を備えた構成例の各アプリケーション
へのスマートカードへのアクセス処理を示す図



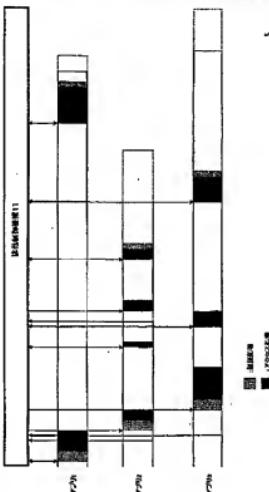
【3】

排他割御機構及びアクセス割御機構を設けた場合の構成図



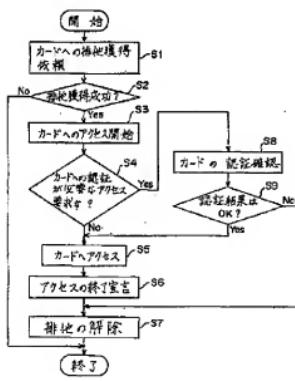
[图 6]

歩他制御機構及びアクセス制御機構を備えた構成時の各アプリケーションへのスマートカードへのアクセス処理を示す図



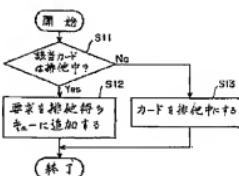
[图7]

スマートカードにアクセスを行なうアプリケーションの処理を示すフローチャート



【圖 8】

アプリケーションからの特徴獲得要求に対する 特徴獲得機能の処理フロー



【図5】

アプリケーションがスマートカードへのアクセスを行う際の、アプリケーション、
持他制御機構及びアクセス制御機構の処理の流れを示した図

持他制御機構11

2)カードaに対し持他制御済みのア
プリがあるか調べ、あれば持他
済みのキーに登録する。なければ、
アプリ1の持他登録をする。

1)カードaに対するアプリ1の持他
登録を解除し、次の待ちがあれば、
それを登録する。

14)2)と同様な処理を行い次の段を
要する。

3)1)と同様な処理を行い、持他
を解除する。

アプリ1

1)カードaへの持他開始

2)カードaへのアクセス開始宣言

3)PIN指定カードaへの認証を
要求する。

4)カードaへのアクセスを行う。

5)一旦、カードの事を解除する
場合に、持他登録を解除する。

6)カードaに対する登録を解消
する。

7)カードaへのアクセスを行う。

8)カードaへの持他開始

9)カードaへの認証を解除する。

10)カードaへの持他登録

11)カードaへのアクセスを行う。

12)カードaへの持他登録

13)カードaへの持他登録

14)カードaへの持他登録

15)カードaへの持他登録

16)カードaへの持他登録

17)カードaへの持他登録

18)カードaへの持他登録

19)カードaへの持他登録

20)スマートカードへのアクセス終了

21)持他登録

22)持他を解除する。

アクセス制御機構12

4)認証は監査管理テーブルにアプリ
1を登録する。

5)カードaに申し、PINを通知し、
確認チェックを行う。

6)認証チェックの結果、OKなら、
監査状態管理テーブルにアプリ1
がカードaに認証済であることを登
録する。

7)認証状態管理テーブルに監査済
し、アプリ1がカードaに認証済なら
カードaにアクセスを行う。

8)認証状態管理テーブルを検査
し、アプリ1がカードaに認証済なら
カードaにアクセスを行う。

9)認証済なら、アプリ1にエラーを
通知する。

10)9)と同様な処理を行う。

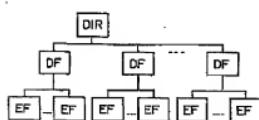
11)アプリ1から、カードa認証済の
情報を削除する。

12)カードaに認証済のアプリ
がなければ、カードaに認証解除を
要求する。

13)認証状態管理テーブルから、
アプリ1を削除する。

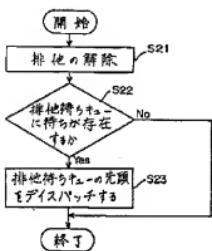
【図15】

スマートカード内部の論理的構成を
示す図



【図9】

アプリケーションからの排他の解除通知に対する排他制御機構の処理を示す
フローチャート



【図10】

アプリケーションからのスマートカードへの
アクセス開始宣言に対するアクセス
制御機構の処理を示すフローチャート

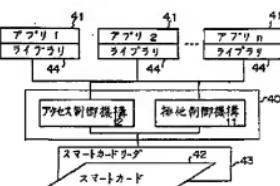
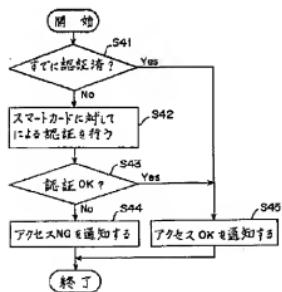


【図12】

本実施形態におけるスマートカードを使用する
システムの構成を示す図

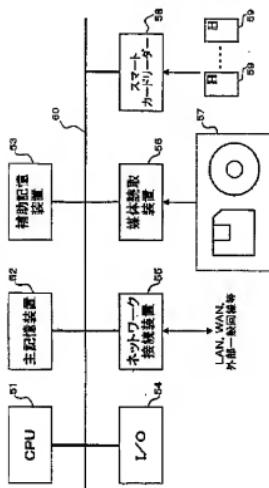
【図11】

アプリケーションからのスマートカードへのアクセス要求に対する
アクセス制御機構の処理を示すフローチャート



【図13】

情報処理のシステム環境図



【図14】

記憶媒体の例を示す図

